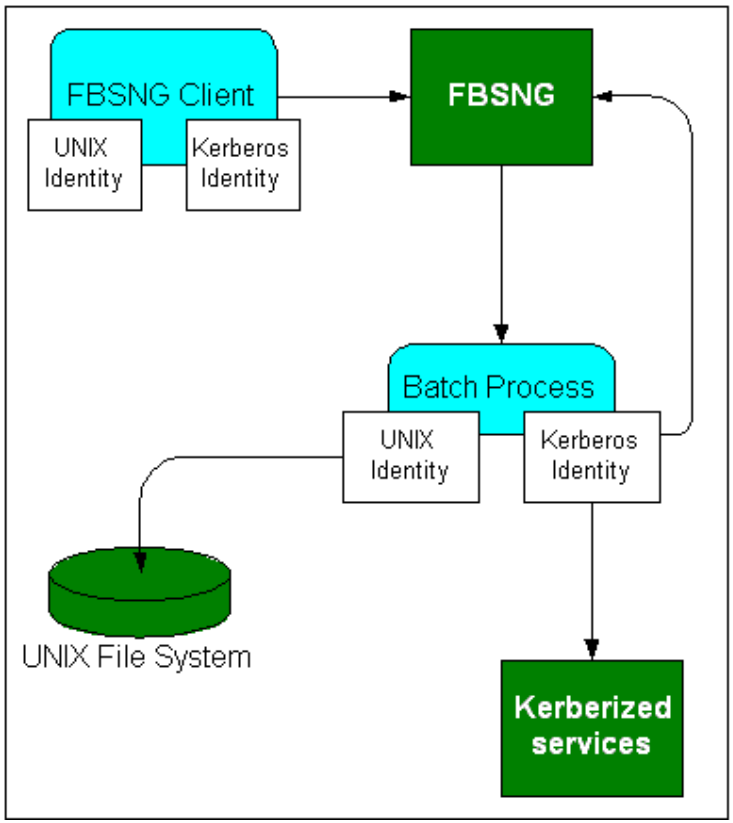
FBSNG and Kerberos

FBSNG Specifics

FBSNG Client Authentication and Authentication



- Authentication – client must prove their (personal) identity
  - Ask the client to present Kerberos credentials
- Authorization – client is granted permission to assume requested UNIX identity
  - Client's identity does not always match UNIX identity
    - E.g. group accounts – many individuals use the same UNIX account
  - UNIX identity (username, UID, GID) used to gain to computational resources
  - FBSNG creates brand new credentials for batch processes so that they in turn may prove their identity to other services

FBSNG Client Authentication

- FBSNG (optionally) uses Kerberos V5 to authenticate clients
- Authentication is required to:
  - Submit jobs
  - Control jobs (hold, release, kill, etc.)
  - Modify farm configuration
- Authentication is skipped for “read-only” operations such as:
  - Get job status
  - Get farm configuration parameters
  - Get resource utilization information

FBSNG Authorization: Proxy Lists

- General authorization request:
  - I am user "X", you have seen my credentials
  - I need to use resources as user "Y"
  - I need my processes to be able to prove "Y" identity
- In simple cases, X = Y
- In case of group accounts, X != Y
- Other services such as rsh, rcp, telnet, etc. use ~Y/.k5login file to determine whether X is allowed to impersonate Y
- FBSNG stores this information in its configuration
  - What if there is no ~Y on one or more nodes ?
- Therefore, group account users must contact FBSNG administrator to declare that "X can represent Y".
- FBSNG "user profile" contains list of Kerberos principals who are granted access to the UNIX account (***proxy list***)
- This is unnecessary for individual accounts (X = Y)

FBSNG Authorization: Special Farm Principals

- Batch processes need to have Kerberos credentials to use kerberized services (rcp, rsh, ftp, etc.)
- Credentials forwarding is not an option because original credentials may expire even before the job starts
- FBSNG creates brand new credentials at the time the job starts
- Impossible to recreate original principal's credentials
  - Group accounts do not have principals
  - Passwords are not to be stored on disk
- Special farm principals look like regular principals but they are not:

  `<user>/<farm name>/farm@<realm>`

  `e.g.: sdssdp/ft/farm@FNAL.GOV`

Batch Job Credentials

- Principal: `<username>/<farm>/farm@<realm>`
  - Username here is username of the batch process, not the name of the principal who submitted the job (X not always = Y)
  - Must be entered into .k5login and/or FBSNG configuration in order to use the services in batch
- Every batch process (not section, not job) receives its individual credentials when it starts
- TGT lifetime: 7 days
- TGT expiration time: 24+ hours
- Stored in file pointed to by $KRB5CCNAME
  - Kerberos standard
  - KRB5CCNAME is set by FBSNG
- For long jobs, must be renewed at least once per 24 hours:

```
(while 1
  sleep 85000      # a little less than 24 hours
  kinit -R
end) &
```

How to submit a job

1. Ask Farm Team to create special farm principal for your account
   - not necessary to submit a job, but needed for the job to be able to use kerberized services
2. If using group account, make sure your principal is in the proxy list for the account
   - See user profile in $FBS_CONFIG

     ```
     %set user_profile <username>
     principals = …
     ```
   - Contact FBSNG administrator
3. Log in to the farm or an FBSNG client computer
4. Issue “setup kerberos”, “setup fbsng”
5. Make sure you have credentials
   - **`klist`** (if it does not show valid credentials – find out why)
     - Were credentials forwarded ?
     - Use **`kinit`** to create credentials
6. Submit the job